

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

Kousetsu SAI

Application No.:

Group Art Unit:

Filed: January 26, 2004

Examiner:

For: SECURITY SYSTEM, INFORMATION MANAGEMENT SYSTEM, ENCRYPTION  
SUPPORT SYSTEM, AND COMPUTER PROGRAM PRODUCT

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith  
a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-51842

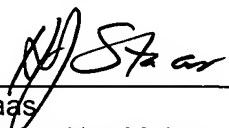
Filed: February 27, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing  
date(s) as evidenced by the certified papers attached hereto, in accordance with the  
requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 26, 2004

By:   
H.J. Staas  
Registration No. 22,010

1201 New York Ave, N.W., Suite 700  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年   2 月 2 7 日  
Date of Application:

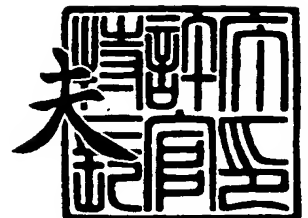
出 願 番 号            特 願 2 0 0 3 - 0 5 1 8 4 2  
Application Number:  
[ST. 10/C] :            [ J P 2 0 0 3 - 0 5 1 8 4 2 ]

出   願   人            富 士 通 株 式 会 社  
Applicant(s):

2 0 0 3 年 1 0 月 1 0 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号   出証特 2 0 0 3 - 3 0 8 3 9 0 1

【書類名】 特許願

【整理番号】 0295715

【提出日】 平成15年 2月27日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明の名称】 セキュリティシステム、情報管理システム、暗号化支援システム、およびコンピュータプログラム

【請求項の数】 5

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 崔 浩哲

【特許出願人】

    【識別番号】 000005223

    【氏名又は名称】 富士通株式会社

【代理人】

    【識別番号】 100086933

    【弁理士】

    【氏名又は名称】 久保 幸雄

    【電話番号】 06-6304-1590

【手数料の表示】

    【予納台帳番号】 010995

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9704487

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティシステム、情報管理システム、暗号化支援システム、およびコンピュータプログラム

【特許請求の範囲】

【請求項 1】

情報を管理する情報管理システムと、前記情報管理システムにおいて情報の暗号化を行うための支援を行う暗号化支援システムと、を有し、

前記暗号化支援システムには、

情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示す規則情報を記憶する暗号化規則記憶手段と、

前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する暗号化用データ送信手段と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理情報受信手段と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、

前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、が設けられ、

前記情報管理システムには、

前記暗号化用データを前記暗号化支援システムより受信する暗号化用データ受信手段と、

当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、

当該情報管理システムが管理する情報の暗号化を、前記暗号化データ受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、

前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、

前記暗号化手段によって行われた暗号化についての前記処理情報を前記暗号化支援システムに送信する処理情報送信手段と、が設けられ、  
てなることを特徴とするセキュリティシステム。

**【請求項 2】**

前記規則情報は、前記規則として、暗号化を行う際に用いる暗号方式と当該暗号化の際に使用する暗号鍵の有効期限とを示し、

前記情報管理システムが情報に暗号化を施した時から現在までの時間が当該情報の区分に対応する前記秘密レベルの前記規則に係る前記有効期限を超えた場合に、

前記警告手段は、当該情報管理システムに対して前記警告を与え、

前記規則情報に示される前記暗号方式が変更された場合に、

前記暗号化用データ送信手段は、当該変更された暗号方式による暗号化を行うための前記暗号化用データを前記情報管理システムに送信し、

前記警告手段は、前記警告として、当該変更された暗号方式に従って情報の暗号化を行うべき旨の警告を与える、

請求項 1 記載のセキュリティシステム。

**【請求項 3】**

暗号化支援システムが提供する、情報の暗号化を行うための支援を受けることによって、情報を管理する情報管理システムであって、

情報を秘密にしたいレベルである秘密レベルごとに定められた、情報の暗号化の規則を示す規則情報と、当該規則に従って情報の暗号化を行うために必要なデータである暗号化用データとを、前記暗号化支援システムより受信する受信手段と、

当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、

当該情報管理システムが管理する情報の暗号化を、前記受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、

前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、

前記規則に従って情報の暗号化が行われたか否かのチェックを受けるために、前記暗号化手段によって行われた暗号化の処理の内容を示す処理情報を前記暗号化支援システムに送信する処理情報送信手段と、  
が設けられてなることを特徴とする情報管理システム。

#### 【請求項 4】

情報を管理する情報管理システムに対して情報の暗号化を行うための支援を行う暗号化支援システムであって、  
情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示す規則情報を記憶する暗号化規則記憶手段と、  
前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する送信手段と、  
前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する受信手段と、  
前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、  
前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、  
が設けられてなることを特徴とする暗号化支援システム。

#### 【請求項 5】

情報を管理する情報管理システムに対して情報の暗号化を行うための支援を行うコンピュータに用いられるコンピュータプログラムであって、  
情報を秘密にしたいレベルである秘密レベルごとの、情報の暗号化の規則を示す規則情報と当該規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する処理と、  
前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理と、  
前記情報管理システムにおいて前記規則に従って情報の暗号化が行われている

か否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う処理と、

前記監視によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える処理と、

をコンピュータに実行させるためのコンピュータプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、機密情報の暗号化管理を行うためのシステムに関する。

【0002】

【従来の技術】

従来より、企業、学校、政府、または自治体などの機関のために、その機関で取り扱われる情報が漏洩しないようにする様々な対策が提案されている。例えば、これらの機関の内部のネットワークと外部のネットワーク（インターネットなど）との間にファイアウォールを設け、外部から内部へのアクセスを制限しまたは禁止する方法が提案されている。

【0003】

ところが、ファイアウォールを設けたとしても、内部のネットワークにセキュリティホールがあると、外部からの攻撃を受け、情報が漏洩してしまうおそれがある。その機関に属するユーザ（職員）が、操作を誤って情報を漏洩してしまう可能性もある。また、職員が不正に情報を漏らしてしまう可能性もないとは言えない。また、改ざんや偽造により、情報の内容そのものの正当性が侵される可能性がある。

【0004】

そこで、暗号化しまたは電子署名を付して情報のデータを取り扱う方法が提案されている。これにより、たとえデータが外部に流出したとしても、暗号を解くことができなければ、その情報の内容を確認することができない。よって、実質的に情報の漏洩を防止することができる。

## 【0005】

## 【発明が解決しようとする課題】

しかし、例えば、複数の支店、営業所、または出張所などの部門を有する大規模な機関において上記の方法を採用するとなると、技術情報（例えば、使用している暗号方式の脆弱性および最新の暗号方式などに関する情報）をチェックすることができかつその技術情報に基づいてセキュリティ対策（セキュリティポリシー）を実行することができる専門の技術者を管理者として部門ごとに配属しなければならない。また、すべての管理者の技術レベルを一定以上に保つ必要がある。そうすると、人件費などのコストが増大してしまう。

## 【0006】

そこで、システムセンターなどにおいて各部門で取り扱う情報を一元管理する方法が考えられる。しかし、そうすると、システムセンターと各部門との通信量が増大し、システムセンターにおける処理の負荷が増大し、また、不正に暗号が解かれた場合のリスクが大きくなる、といった問題点が生じる。

## 【0007】

このような事情により、大規模な機関において上記の暗号化の方法の活用が上手く図れていないことが多い。

一方、小規模な機関（例えば、S O H O など）においても、上記の暗号化の方法の活用が進んでいないことが多い。暗号化に関する技術情報を得ることやセキュリティ対策を行うことは難しく、実際にこれらの作業を行っても、取り扱う情報の量が少ないと割に合わないからである。

## 【0008】

そこで、情報管理を外部の業者に委託（アウトソーシング）することが考えられる。しかし、その業者から情報が漏洩するおそれがないとは必ずしも言えないので、重要な機密情報は手元に置いて管理したいと思う経営者が多い。

## 【0009】

本発明は、上記のような問題点に鑑み、部門ごとに自らの情報を管理しつつ、高水準のセキュリティの維持を容易に図ることを目的とする。

## 【0010】



**【課題を解決するための手段】**

本発明に係るセキュリティシステムは、情報を管理する情報管理システムと、前記情報管理システムにおいて情報の暗号化を行うための支援を行う暗号化支援システムと、を有する。前記暗号化支援システムには、情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示す規則情報を記憶する暗号化規則記憶手段と、前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する暗号化用データ送信手段と、前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理情報受信手段と、前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、を設ける。前記情報管理システムには、前記暗号化用データを前記暗号化支援システムより受信する暗号化用データ受信手段と、当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、当該情報管理システムが管理する情報の暗号化を、前記暗号化データ受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、前記暗号化手段によって行われた暗号化についての前記処理情報を前記暗号化支援システムに送信する処理情報送信手段と、を設ける。

**【0011】**

好ましくは、前記規則情報は、前記規則として、暗号化を行う際に用いる暗号方式と当該暗号化の際に使用する暗号鍵の有効期限とを示し、前記情報管理システムが情報に暗号化を施した時から現在までの時間が当該情報の区分に対応する前記秘密レベルの前記規則に係る前記有効期限を超えた場合に、前記警告手段は、当該情報管理システムに対して前記警告を与え、前記規則情報に示される前記暗号方式が変更された場合に、前記暗号化用データ送信手段は、当該変更された

暗号方式による暗号化を行うための前記暗号化用データを前記情報管理システムに送信し、前記警告手段は、前記警告として、当該変更された暗号方式に従って情報の暗号化を行うべき旨の警告を与える。

#### 【0012】

または、情報に対して電子署名を行うための証明書の有効期限を管理する有効期限管理手段を設け、前記監視手段は、前記証明書の有効期限に基づいて、情報に対して電子署名をやり直す必要があるか否かを監視し、前記警告手段は、電子署名をやり直す必要があると判別された場合に、当該情報を管理する前記情報管理システムに対して電子署名をやり直すべき旨の警告を与える。

#### 【0013】

または、前記情報管理システムに、当該情報管理システムが管理する情報の区分と当該区分に対応する前記秘密レベルとを示す区分秘密レベル情報を前記暗号化支援システムに送信する区分秘密レベル送信手段を設ける。そして、前記監視手段は、情報管理システムより受信した前記処理情報と前記区分秘密レベル情報とを比較することによって前記監視を行う。

#### 【0014】

##### 【発明の実施の形態】

図1は本発明に係るセキュリティシステム1の構成の例を示す図、図2は機密情報サーバ31のハードウェア構成の例を示す図、図3は機密情報サーバ31の機能的構成の例を示す図、図4はポリシー管理サーバ21の機能的構成の例を示す図、図5は暗号化ランクテーブルTB4の例を示す図、図6は機密情報グループテーブルTB5の例を示す図、図7は部署メンバーテーブルTB6の例を示す図、図8は署名期限テーブルTB7の例を示す図、図9は作成データ管理テーブルTB0の例を示す図、図10はシステム管理部門が有する例外属性テーブルTB8の例を示す図、図11はある営業所Mが有する例外属性テーブルTB9の例を示す図、図12は顧客連絡先テーブルTB1の例を示す図、図13は検針情報テーブルTB2の例を示す図、図14は料金支払テーブルTB3の例を示す図、図15は暗号化および電子署名の処理の手順の例を示す図である。

#### 【0015】

本発明に係るセキュリティシステム 1 は、図 1 に示すように、暗号化支援システム 2、機密情報管理システム 3、およびネットワーク 4 などによって構成される。暗号化支援システム 2 と機密情報管理システム 3 とは、ネットワーク 4 を介して互いに接続可能である。ネットワーク 4 として、イントラネット、インターネット、公衆回線、または専用線などが用いられる。また、暗号化支援システム 2 と機密情報管理システム 3 との間には認証が成立していることが望ましい。

#### 【0016】

このセキュリティシステム 1 は、例えば、複数の営業所または支店などの部門を有する会社または複数の支所または出張所などの部門を有する行政機関などに設けられる。以下、複数の営業所を有する会社 X に設けられたセキュリティシステム 1 を例に説明する。

#### 【0017】

機密情報管理システム 3 は、機密情報サーバ 31 および端末装置 32 などによって構成される。この機密情報管理システム 3 は、営業所ごとに設けられており、その営業所の顧客情報、研究中の技術に関する情報、営業活動などのノウハウ、他社についての調査報告、財務情報、および人事情報など、種々の機密情報（社外秘情報）の管理を行う。

#### 【0018】

これらの機密情報には、暗号化および電子署名の処理が施されている。また、これらの機密情報は、機密情報サーバ 31 において、テキストエディタ、ワープロソフト、表計算ソフト、またはグラフィックソフトなどで作成されたテキストファイルまたはバイナリファイルとして管理され、またはデータベースのレコードとして管理される（図 12、図 13、図 14 参照）。以下、これらのファイルまたはレコードつまり機密情報のデータを「機密データ S D T」と記載する。

#### 【0019】

機密情報サーバ 31 は、図 2 に示すように、CPU 31a、RAM 31b、ROM 31c、磁気記憶装置 31d、ディスプレイ装置 31e、マウスまたはキーボードなどの入力装置 31f、および各種インタフェースなどによって構成される。磁気記憶装置 31d には、オペレーティングシステム（OS）および後に示

す各機能を実現するためのプログラムおよびデータなどがインストールされている。これらのプログラムおよびデータは、CD-ROMなどの記録媒体によって提供されまたはポリシー管理サーバ21によってネットワーク4を介して提供される。そして、必要に応じてRAM31bにロードされ、CPU31aによってプログラムが実行される。

#### 【0020】

このような構成によって、機密情報サーバ31には、図3に示すように、ポリシー適用部302、暗号化実行部303、署名処理実行部304、機密情報更新部305、グループ情報通知部306、アクセスログ通知部307、インデックス管理部308、メンバー情報通知部309、暗号ポリシーデータベース3D1、機密情報グループデータベース3D2、例外属性データベース3D3、メンバーグループデータベース3D4、機密情報データベース3D5などの機能が実現される。

#### 【0021】

端末装置32は、営業所の各部署に1台または複数台設置されており、その営業所に配属されている社員が機密情報を取り扱うために使用される。ただし、社員ごとに機密情報の使用権限（アクセス権）が設定されている。これについては、後に説明する。

#### 【0022】

暗号化支援システム2は、ポリシー管理サーバ21および端末装置22などによって構成される。この暗号化支援システム2は、会社Xのシステムを統括するシステム管理部門などによって管理されている。ポリシー管理サーバ21は、各営業所の機密情報管理システム3において行われる機密データSDTのセキュリティ管理のための、支援に関する処理を行う。端末装置22は、システム管理部門の管理者がポリシー管理サーバ21の操作を行うために用いられる。システム管理部門は、セキュリティを統括して管理する権限を有していればよく、専任であるか兼任であるかは問わない。

#### 【0023】

ポリシー管理サーバ21は、図2に示す機密情報サーバ31と同様のハードウ

ェア構成をしており、図 4 に示すようなポリシー情報配付部 2 0 2、適用状況監視部 2 0 3、適用状況集計部 2 0 4、適用警告部 2 0 5、脆弱性監視部 2 0 6、例外属性送信部 2 0 7、暗号ポリシーデータベース 2 D 1、機密情報グループデータベース 2 D 2、例外属性データベース 2 D 3、メンバーグループデータベース 2 D 4、およびアクセスログデータベース 2 D 5 などの機能が実現される。

#### 【0 0 2 4】

以下、図 3 に示す機密情報サーバ 3 1 および図 4 に示すポリシー管理サーバ 2 1 の各部の機能について、機密データ S D T のセキュリティ管理のための機能とそれを実現する準備のための機能とに大別して説明する。

#### 【0 0 2 5】

〔セキュリティ管理の準備のための機能〕

会社 X では、自社のセキュリティ方策（セキュリティポリシー）および個人情報保護方策（個人情報保護ポリシー）の一環として暗号ポリシーを定めている。

「暗号ポリシー」とは、機密情報のデータ（機密データ S D T）を暗号化する際に守らなければならない規則、取決め、および方策などを意味するものである。会社 X は、自社の暗号ポリシーとして、機密情報の重要性または秘密性（秘匿性）などの大きさに応じた幾つかのランク（レベル）を定めている。以下、これを「暗号化ランク」と記載する。そして、この暗号化ランクごとに暗号化のルールを定めている。

#### 【0 0 2 6】

例えば、図 5 に示すように、暗号化ランク A、B、…ごとに、暗号化のルールとして、暗号方式および更新頻度を定めている。「暗号方式」とは、機密データ S D T を暗号化する際に用いる暗号技術のことである。例えば、D E S（Data Encryption Standard）、3 D E S、F E A L（Fast Data Encipherment Algorithm）、I D E A（International Data Encryption Algorithm）、または R S A（Rivest Shamir Adleman）などの暗号技術が用いられる。「更新頻度」とは、暗号化をやり直す頻度つまり周期を意味する。例えば、「6 0 日」と定められている場合は、6 0 日以内ごとに新たな暗号鍵を生成し、その暗号鍵によって暗号化をやり直さなければならない。

**【0027】**

なお、本実施形態において、図5の「暗号化ランク」のランク（レベル）は、全体的に見てA、B、…の順に暗号の解読が難しくなる傾向を示しているが、常に暗号の解読の困難性を示すものではない。上に説明したように、本実施形態の暗号化ランクは、「暗号方式」および「更新頻度」などを組み合わせた暗号化のルールを識別するために用いられる。もちろん、他の実施形態として、暗号化ランクを暗号の解読の困難性を示すものとして用いることも可能である。

**【0028】**

ポリシー管理サーバ21（システム管理部門）の管理者は、端末装置22を操作するなどして、各暗号化ランクの暗号化のルールを入力し、図5に示す暗号化ランクテーブルTB4を作成する。この際に、会社Xで取り扱われる各機密情報の機密データSDTをいずれの暗号化ランクのルールに基づいて暗号化すべきであるかを定める。そして、各暗号化ランクに属する機密情報の区分（属性、クラス）の名称を「機密情報」のフィールドに指定する。なお、本実施形態では、機密情報の区分のために、その機密情報の機密データSDTが格納場所であるテーブルまたはディレクトリが用いられる。

**【0029】**

図4の暗号ポリシーデータベース2D1は、作成された暗号化ランクテーブルTB4を記憶し管理する。また、各暗号方式（ $\alpha$ 、 $\beta$ 、…）ごとに、その暗号方式に基づいて暗号化を行うために必要な暗号化用データDT5を記憶する。暗号化用データDT5の形態として、その暗号方式を実行するためのメインプログラムファイルまたはその暗号方式に用いられる関数または数値などのデータファイル（いわゆるライブラリ）などがある。

**【0030】**

ポリシー情報配付部202は、暗号化ランクテーブルTB4および暗号化用データDT5を各営業所の機密情報サーバ31に送信することによって、会社Xの暗号ポリシーの情報を配付する。暗号化ランクテーブルTB4の内容が更新された場合は、新しい暗号化ランクテーブルTB4を配付する。この場合は、更新された個所（レコード）だけを配付するようにしてもよい。暗号化用データDT5

が更新または追加された場合も、その新たな暗号化用データDT5を各機密情報サーバ31に配付する。

#### 【0031】

図3のポリシー適用部302は、ポリシー管理サーバ21から送信されてきた暗号化ランクテーブルTB4を暗号ポリシーデータベース3D1に記憶させ、暗号化用データDT5を所定のディレクトリに格納する。つまり、機密情報サーバ31に会社Xの暗号ポリシーを適用し、この暗号ポリシーに基づいて暗号化の処理を実行することができるように、プログラムおよびデータのインストールを行う。更新された暗号化用データDT5または暗号化ランクテーブルTB4のレコードが送信されてきた場合は、対応する古い暗号化用データDT5またはレコードと置き換える。

#### 【0032】

機密情報グループデータベース3D2は、図6に示すような機密情報グループテーブルTB5を記憶し管理する。サーバIDは、機密データSDTが格納されている装置つまり機密情報サーバ31を識別するためのIDである。機密情報グループG1、G2、…は、それぞれ、機密情報サーバ31で管理される機密データSDTのうちの使用権限の与えられた利用者グループ（部署）が同一でありかつ暗号化ランクが同一である機密データSDTの区分をグループ化したものである。

#### 【0033】

例えば、機密情報グループテーブルTB5の第一レコード（サーバID=S001、機密情報グループ=G1）によると、営業所Mの料金支払テーブルTB3（図14参照）および検針情報テーブルTB2（図13参照）に格納される機密情報の機密データSDTが、「暗号化ランク=C」に対応する暗号方式によって暗号化され、かつ、第1課（顧客窓口の部署）の社員に対して使用する権利が与えられていることが、分かる。どの機密情報がどの機密情報グループに属するのかは、ポリシー管理サーバ21から取得した暗号化ランクテーブルTB4（図5参照）に示される暗号ポリシーに従って、営業所ごとに定められる。

#### 【0034】

なお、暗号化ランクテーブル T B 4 において、「ランク = C」のように 1 つの暗号化ランクに複数の暗号方式が対応付けられている場合がある。この場合は、その営業所の管理者が機密情報の使用の利便性などに応じていずれか 1 つの暗号方式を選択し、機密情報グループテーブル T B 5 に指定すればよい。または、機密情報管理システム 3 の環境（例えば、機密情報管理システム 3 のネットワークの設定情報、機密情報サーバ 3 1 の O S の堅牢性、またはその機密情報の使用頻度など）に基づいて、いずれかの暗号方式を自動的に選択するように構成してもよい。また、「他社秘密情報」のように暗号化ランクが複数ある機密情報については、その営業所の管理者が、機密情報ごとにその秘匿性または重要性などに応じていずれかの暗号化ランクを選択すればよい。

#### 【 0 0 3 5 】

機密情報グループテーブル T B 5 の「暗号化ビット数」は、その機密情報グループの暗号方式による暗号化の際に用いられる暗号鍵のサイズを示す。「レコード数」は、その機密情報グループに属する項目（区分）の機密データ S D T の総数である。

#### 【 0 0 3 6 】

図 3 のグループ情報通知部 3 0 6 は、上記のように定められた機密情報グループテーブル T B 5 をポリシー管理サーバ 2 1 に送信することによって、各機密情報の機密データ S D T をどのように暗号化するのかをシステム管理部門に通知する。つまり、営業所のローカルの暗号ポリシーを通知する。図 4 の機密情報グループデータベース 2 D 2 は、各営業所から送信されてきた機密情報グループテーブル T B 5 を記憶し管理する。

#### 【 0 0 3 7 】

図 3 のメンバーグループデータベース 3 D 4 は、図 7 に示す部署メンバーテーブル T B 6、図 8 に示す署名期限テーブル T B 7、および図 9 に示す作成データ管理テーブル T B 0（T B 0 a、T B 0 b、…）を記憶し管理する。

#### 【 0 0 3 8 】

部署メンバーテーブル T B 6 には、機密情報サーバ 3 1 の利用者すなわち営業所の各部署の社員の一覧が格納されている。署名期限テーブル T B 7 には、その



社員それぞれの電子署名用の署名鍵の有効期限を示す情報が格納されている。作成データ管理テーブルTB0は、社員（メンバー）ごとに1つずつ設けられ、その社員が署名した文書（機密データSDT）の文書IDを格納する。

#### 【0039】

メンバー情報通知部309は、部署メンバーテーブルTB6、署名期限テーブルTB7、および作成データ管理テーブルTB0をポリシー管理サーバ21に送信することによって、営業所の社員の情報をシステム管理部門に通知する。図4のメンバーグループデータベース2D4は、各営業所から送信されてきた部署メンバーテーブルTB6、署名期限テーブルTB7、および作成データ管理テーブルTB0を記憶し管理する。

#### 【0040】

前に述べたように、機密データSDTの暗号化を行う際のルールは営業所ごとに図6の機密情報グループテーブルTB5によって定められているが、システム管理部門（暗号化支援システム2）は、この暗号化のルールの例外を、図10に示す例外属性テーブルTB8によって定めることができる。

#### 【0041】

例えば、図5の暗号化ランクテーブルTB4に示すように、会社Xの暗号ポリシーによると、各営業所は、社内人事に関する機密情報の機密データSDTを「暗号化ランク=B」と設定しなければならない。そこで、ある営業所（例えば、営業所M）では、図6に示すように、社内人事情報テーブルに格納される機密データSDTの暗号化ランクを「B」に設定している。しかし、システム管理部門は、このルールの例外として、図10の例外属性テーブルTB8のように、営業所Mの社内人事情報テーブルについて「暗号化ランク=A」と設定することができる。また、1つの営業所単位で指定するだけでなく、「全社」の「料金支払テーブル」のように複数の営業所をまとめて指定することも可能である。これにより、複数の営業所に共通する機密情報の区分の暗号化ランクを一時的に一斉に設定することができる。

#### 【0042】

このような例外の設定は、例えば、次のような場合に行えばよい。例えば、そ

の営業所の機密情報管理システム 3 の中にセキュリティホールが見つかった場合、その営業所の社員のパスワードまたは暗号鍵が漏洩するなどして特定の機密データ S D T への不正なアクセスの危険性が高まった場合、または実際に不正なアクセスが行われたために特定の営業所または不特定の営業所に対して機密データのセキュリティが保証されない状況が発生したと考えられる場合などである。これにより、効率的にセキュリティを高めることができる。

#### 【0043】

この例外属性テーブル T B 8 は、図 4 の例外属性データベース 2 D 3 によって記憶され管理される。そして、例外を示す各レコードは、例外情報 D T 4 として、その例外が与えられた営業所に対して例外属性送信部 2 0 7 によって送信される。各営業所の例外属性データベース 3 D 3（図 3 参照）は、送信されてきた例外情報 D T 4 を例外属性テーブル T B 9 に格納し管理する。例えば、営業所 M では、図 1 1 に示すように、受信した例外情報 D T 4 が格納される。

#### 【0044】

機密情報データベース 3 D 5 は、機密情報の機密データ S D T を、レコードとしてテーブルに格納し管理する。または、ファイルとして磁気記憶装置 3 1 d（図 2 参照）の所定のディレクトリに格納し管理する。会社 X が電力会社である場合は、例えば、図 1 2 に示す顧客連絡先テーブル T B 1 にはから電力の供給などのサービスを受ける顧客の連絡先を示す機密データ S D T が格納され、図 1 3 に示す検針情報テーブル T B 2 には顧客が使用した電力量（検針値）を示す機密データ S D T が格納され、図 1 4 には電気料金の支払方法に関する機密データ S D T が格納される。これらの機密データ S D T は、次に説明するような暗号化および電子署名の処理が施された上で管理される。

#### 【0045】

〔セキュリティ管理（暗号化および電子署名）のための機能〕

暗号化実行部 3 0 3 および署名処理実行部 3 0 4 は、図 6 に示す機密情報グループテーブル T B 5 および図 1 1 に示す例外属性テーブル T B 9 を参照し、それぞれ、機密データ S D T の暗号化の処理および電子署名の処理を行う。これらの処理は、例えば、図 1 5 に示すような流れで行われる。

**【 0 0 4 6 】**

署名処理実行部 3 0 4 は、機密データの作成者または承認者などに対応付けられて設定されている署名方式によって電子署名を生成するとともに（# 1）、タイムスタンプ（TST : Time Stamp Token）を受け取る（# 2）。電子署名の生成は、例えば、ハッシュ関数によって機密データ S D T を圧縮し暗号化することによって行う。ハッシュ関数として、MD 5（Message Digest Algorithm 5）、S H A - 1（Secure Hash Algorithm 1）、または H M A C（Hashed Based Message Authentication Code）などが用いられる。

**【 0 0 4 7 】**

暗号化実行部 3 0 3 は、機密情報グループデータベース 3 D 2 に記憶されている図 6 の機密情報グループテーブル T B 5 を参照し、電子署名および T S T が添付された機密データ S D T を暗号化する（# 3）。例えば、作成したプログラムのソースファイルを機密データ S D T としてソースファイルディレクトリに格納する場合は、σ 暗号方式によって暗号化を行う。

**【 0 0 4 8 】**

ただし、図 1 1 の例外属性テーブル T B 9 に暗号化の例外が設定されている機密情報の機密データ S D T については、この例外に示される暗号化ランクの暗号方式によって暗号化を行う。

**【 0 0 4 9 】**

ステップ # 3 で用いられる暗号鍵は、例えば、その営業所または部署ごとにフロッピディスクなどの記録媒体に保存（記録）され管理される。そして、暗号化を行うごとに機密情報サーバ 3 1 にロードして用いられる。また、署名鍵は、機密データ S D T を作成しまたは更新した本人のものが用いられ、普段は本人が所持する I C カードなどに記録されている。

**【 0 0 5 0 】**

電子署名および T S T が添付され暗号化された機密データ S D T は、機密情報データベース 3 D 5 によって管理される（# 4）。なお、暗号化および電子署名の処理が完了すると、処理が完了した旨、処理対象、および使用した暗号方式および署名方式などを示す処理完了情報 D T 1 をポリシー管理サーバ 2 1 に送信す

る。また、機密情報グループテーブルTB5（図6参照）の「レコード数」を修正する。さらに、機密データSDTの作成者の作成データ管理テーブルTB0（図9参照）にその機密データSDTの文書IDを追加する。

#### 【0051】

図3に戻って、機密情報更新部305は、機密情報データベース3D5で管理されている機密情報の内容つまり機密データSDTを更新するための処理を行う。まず、暗号化されている機密データSDTを復号し、その内容を端末装置32のディスプレイ装置に表示する。社員による内容の修正の操作を受け付ける。そして、暗号化実行部303および署名処理実行部304に対して、暗号化および電子署名の処理を行うように指令する。これにより、更新された機密データSDTに対して、図15に示す処理が再度施される。この機密データSDTは、更新前の機密データSDTと置き換えられる。なお、修正（更新）が行われなかった場合つまり機密情報の閲覧のみ行われた場合は、閲覧が終わった後、復号された機密データSDTは破棄され、元の機密データSDTがそのまま残される。

#### 【0052】

アクセスログ通知部307は、機密データSDTへのアクセスがあったときに、その日時、その機密データSDTの属する機密情報グループ、およびアクセスした社員などに関するログ情報LDTをポリシー管理サーバ21に通知する。例えば、機密データSDTの内容が修正（更新）されまたは閲覧されたときに、ログ情報LDTを通知する。また、アクセスを試みたが失敗した場合も、その旨を示すログ情報LDTを通知する。

#### 【0053】

図4のアクセスログデータベース2D5は、各営業所の機密情報サーバ31から送信されてきたログ情報LDTを記憶し管理する。この際に、営業所ごとに識別コードを割り振り、ログ情報LDTに送信元の営業所の識別コードを対応付けておく。これらのログ情報LDTは、例えば、機密データSDTへの不正なアクセスがあった場合に犯人などを特定するために用いられる。

#### 【0054】

図3のインデックス管理部308は、機密情報データベース3D5が管理する

各テーブル（図 1 2、図 1 3、図 1 4 参照）および各ディレクトリに格納されている暗号化された機密データ S D T に関するインデックスを作成し、管理する。例えば、機密データ S D T の格納場所を示すテーブル名またはディレクトリ名、暗号方式、署名方式、作成者または更新者、または作成日または更新日などを示すインデックスを作成し、管理する。

#### 【 0 0 5 5 】

図 4 の適用状況監視部 2 0 3 は、各営業所の機密情報サーバ 3 1 における暗号ポリシーの適用の状況の監視を行う。監視は、営業所の機密情報サーバ 3 1 から送信されてきた処理完了情報 D T 1 とその営業所の機密情報グループテーブル T B 5 -（図 6 参照）および例外属性テーブル T B 8（図 1 0 参照）とを比較することによって行う。

#### 【 0 0 5 6 】

例えば、機密情報グループテーブル T B 5 に指定されるすべての機密情報の区分に対応する処理完了情報 D T 1 が揃い、かつ、これらの処理完了情報 D T 1 が機密情報グループテーブル T B 5 に指定される暗号方式および署名方式を示していることが確認できた場合は、暗号ポリシーが正しく適用されていると判別する。所定の期間が経過しても処理完了情報 D T 1 が揃わない場合または指定される暗号方式または署名方式とは異なる方式で処理が行われたと確認された場合は、暗号ポリシーが正しく適用されていないと判別する。ただし、指定される暗号方式とは異なる方式で処理が行われた場合であっても、例外属性テーブル T B 8 に示される例外に基づいて処理が行われた場合は、暗号ポリシーが正しく適用されていると判別する。

#### 【 0 0 5 7 】

適用状況集計部 2 0 4 は、適用状況監視部 2 0 3 による監視の結果を集計し、ディスプレイ装置に表示しまたはレポートとして用紙に印刷し、システム管理部門または各営業所の管理者などに知らせる。

#### 【 0 0 5 8 】

適用警告部 2 0 5 は、暗号ポリシーが正しく適用されていないと判別された場合に、その営業所に対して、直ちに暗号ポリシーを正しく適用すべき旨のメッセ

ージを送信することによって警告を行う。

#### 【0059】

適用状況監視部 2 0 3 は、図 5 の暗号化ランクテーブル T B 4 に示される暗号化を行う周期（更新頻度）および図 8 の署名期限テーブル T B 7 に示される電子署名に使用される証明書（以下、単に「電子署名」と記載する。）の有効期限の監視を行う。そして、前に暗号化を行った時点から「更新頻度」フィールドに示される時間が過ぎた場合は、適用警告部 2 0 5 は、対応する機密情報の機密データ S D T の暗号化をやり直すべき旨の警告を行う。電子署名の有効期限が過ぎた場合は、対応する機密情報の機密データ S D T に新たな電子署名を付すべき旨の警告を行う。なお、これらの周期または期限が来る所定の期間前（例えば 1 週間前）に予告のメッセージを送信するようにしてもよい。

#### 【0060】

脆弱性監視部 2 0 6 は、ネットワークに関するサービスを提供する機関など（コンピュータメーカ、通信機器メーカ、インターネットサービスプロバイダ、またはセキュリティサービス会社など）から暗号化および電子署名などに関する技術情報を取得し、機密情報管理システム 3 で用いられている暗号化および電子署名の脆弱性に関する監視を行う。つまり、現在採用している暗号方式などが妥当なものであるか否かの監視を行う。技術情報は、例えば、脆弱性定義ファイルとして提供される。脆弱性の監視は、この脆弱性定義ファイルの内容と図 5 に示す暗号化ランクテーブル T B 4 に定義される暗号方式とをマッチングすることによって行う。

#### 【0061】

脆弱性が発見された場合は、システム管理部門の管理者に対して警告を行う。このとき、管理者は、直ちに脆弱性をなくすための対策を講じる。例えば、各営業所の管理者に対して注意を促す、暗号化レベルを上げる、暗号鍵を交換する、または新たな暗号方式などを採用する、などの対策を講じる。また、ポリシー情報配付部 2 0 2 は、必要に応じて、脆弱性を解決するための新たな暗号化用データ D T 5 または暗号化ランクテーブル T B 4（図 5 参照）を各機密情報管理システム 3 に配付する。

**【0 0 6 2】**

図 1 6 は暗号化および電子署名の処理の流れの例を説明するフローチャート、図 1 7 はシステム管理部門側の準備の処理の流れの例を説明するフローチャート、図 1 8 は営業所側の準備の処理の流れの例を説明するフローチャート、図 1 9 は運用開始後の処理の流れの例を説明するフローチャート、図 2 0 は機密情報へのアクセス要求があった場合の機密情報サーバ 3 1 における処理の流れの例を説明するフローチャート、図 2 1 は各種設定の変更があった場合の機密情報サーバ 3 1 における処理の流れの例を説明するフローチャートである。

**【0 0 6 3】**

次に、ポリシー管理サーバ 2 1 および機密情報サーバ 3 1 における処理の流れを、フローチャートを参照して説明する。各営業所において会社 X のセキュリティポリシーに適合した機密情報の管理を実現するために、ポリシー管理サーバ 2 1 および機密情報サーバ 3 1 は、それぞれ、図 1 6 ( a ) および図 1 6 ( b ) に示すような手順で処理を行う。

**【0 0 6 4】**

ポリシー管理サーバ 2 1 は、各営業所の機密情報の機密データ S D T の暗号化および電子署名の支援のための準備を行う ( # 1 1 ) 。すなわち、図 1 7 に示すように、会社 X のセキュリティポリシーに基づいて策定された暗号ポリシーを入力し ( # 1 1 1 ) 、図 5 に示すような暗号化リンクテーブル T B 4 を作成する ( # 1 1 2 ) 。また、暗号化および電子署名の処理を行うために必要なメインプログラムおよびライブラリなどのデータ ( 暗号化用データ D T 5 ) を用意する ( # 1 1 3 ) 。そして、これらの暗号化リンクテーブル T B 4 および暗号化用データ D T 5 を各営業所の機密情報サーバ 3 1 に送信する ( # 1 1 4 ) 。

**【0 0 6 5】**

一方、機密情報サーバ 3 1 は、その営業所の機密データ S D T の暗号化および電子署名のための準備を行う ( # 2 1 ) 。すなわち、図 1 8 に示すように、ポリシー管理サーバ 2 1 から送信されてきた暗号化リンクテーブル T B 4 および暗号化用データ D T 5 をインストールする ( # 2 1 1 ) 。

**【0 0 6 6】**

機密情報を扱う社員のうち図 7 に示す部署メンバーテーブル T B 6 に登録されていない者がいる場合は（# 2 1 2 で Y e s）、その者を部署メンバーテーブル T B 6 に追加する（# 2 1 3）。併せて、その者に対して署名鍵を発行し、発行された署名鍵に含まれる有効期限を取得し、図 8 に示す署名期限テーブル T B 7 にその署名鍵の有効期限を設定する（# 2 1 4）。

#### 【 0 0 6 7 】

また、暗号方式、署名方式、およびアクセス権の設定がなされていない機密情報の区分がある場合は（# 2 1 5 で Y e s）、図 6 に示す機密情報グループテーブル T B 5 にそれらの設定を行う（# 2 1 6）。つまり、機密情報グループの設定を行う。

#### 【 0 0 6 8 】

そして、図 6、図 7、および図 8 の各テーブルをポリシー管理サーバ 2 1 に送信することによって、その営業所における暗号化のルールおよび社員の情報をシステム管理部門に通知する（# 2 1 7）。

#### 【 0 0 6 9 】

図 1 6 に戻って、機密情報サーバ 3 1 は、図 6 に示す機密情報グループテーブル T B 5 に基づいて、機密データ S D T の暗号化および電子署名の処理を行い（# 2 2）、その処理内容を示す処理完了情報 D T 1 をポリシー管理サーバ 2 1 に送信する（# 2 3）。

#### 【 0 0 7 0 】

ポリシー管理サーバ 2 1 は、各営業所の暗号ポリシーの適用状況の集計を行う（# 1 2）。集計は、その営業所から受信した処理完了情報 D T 1 と機密情報グループテーブル T B 5（図 6 参照）および例外属性テーブル T B 8（図 1 0 参照）とを比較することによって行う。全営業所についての集計が完了すれば、その結果をディスプレイ装置に表示またはレポートとして印刷する。なお、一部の営業所についてのみ集計を行ってもよい。

#### 【 0 0 7 1 】

集計の結果、所定の期間を経過してもなお暗号ポリシーの適用がなされていない場合は（# 1 3 で N o）、その営業所に対して警告メッセージを送信する（#



14)。

#### 【0072】

警告を受けた営業所の機密情報サーバ31は、暗号ポリシーが正しく適用されるように、ステップ#22、#23の処理をやり直す(#24でYes)。また、必要に応じて、機密情報グループ(図6参照)または利用者グループ(図7参照)などの設定をやり直す(#21)。そして、ポリシー管理サーバ21によって、暗号ポリシーの適用がなされていることが確認されれば(#13でYes)、その営業所の暗号ポリシーの適用が完了する(#24でNo)。

#### 【0073】

暗号ポリシーの適用が完了した後、ポリシー管理サーバ21は、図19に示すように、暗号化に用いられた暗号鍵および電子署名に用いられた署名鍵の有効期限(図5、図8参照)の監視、および暗号方式などの脆弱性の監視を行う(#31)。

#### 【0074】

監視によって暗号鍵または署名鍵の有効期限切れが見つかった場合は、その暗号鍵または署名鍵を使用している営業所に対して、暗号化または電子署名の処理を再度行うように指示する(#32)。または、有効期限が切れる所定の期間前に予告するようにしてもよい。

#### 【0075】

監視によって脆弱性が見つかった場合は、各営業所に対して注意を促す。また、必要に応じて、暗号化または電子署名をやり直すように指示し、そのための支援を行う(#32)。つまり、脆弱性に対処した新しい暗号化用データDT5または暗号化ランクテーブルTB4(図5参照)を各機密情報サーバ31に送信し、これに基づいて暗号化または電子署名のやり直しをさせる。特定の営業所に脆弱性が見つかった場合は、例外属性テーブルTB8に暗号化ランクの例外を設定し、その設定の内容(図11参照)をその営業所に送信する。

#### 【0076】

指示または予告を受けた営業所の機密情報サーバ31は、新しい暗号鍵または署名鍵を生成し、暗号化または電子署名の処理をやり直す(#42)。ただし、

新しい暗号化用データ D T 5、新しい暗号化ランクテーブル T B 4、または暗号化ランクの例外を受信した場合は、これらをインストールしてから（# 4 1）、ステップ # 4 2 の処理を行う。暗号化ランクテーブル T B 4（図 5 参照）に変更があった場合は、必要に応じて機密情報グループテーブル T B 5（図 6 参照）の内容を修正し、これに基づいてステップ # 4 2 の処理を行う。そして、処理が完了した旨をポリシー管理サーバ 2 1 に通知する（# 4 3）。

#### 【0077】

ポリシー管理サーバ 2 1 は、図 1 6（a）のステップ # 1 2 ～ # 1 4 と同様に、暗号ポリシーの適用状況を集計し、正しく適用されていない営業所に対して警告を行う（# 3 4 で N o、# 3 5）。警告を受けた営業所の機密情報サーバ 3 1 は、ステップ # 4 1 ～ # 4 3 の処理をやり直す（# 4 4 で Y e s）。

#### 【0078】

暗号化された機密情報の機密データ S D T へのアクセス要求があった場合は、機密情報サーバ 3 1 は、図 2 0 に示すように、要求元のユーザ（社員）にアクセス権があるか否かを機密情報グループテーブル T B 5（図 6 参照）に基づいて判別する（# 5 1）。

#### 【0079】

アクセス権がある場合は（# 5 1 で Y e s）、その機密データ S D T を復号し、その社員に対して表示する（# 5 2）。機密データ S D T の内容が更新された場合は（# 5 3）、更新後の機密データ S D T に対して暗号化および電子署名の処理を行い（# 5 4）、更新があった旨を示すログ情報 L D T をポリシー管理サーバ 2 1 に送信する（# 5 5）。アクセス権がない場合は（# 5 1 で N o）、アクセスの試みがあった旨を示すログ情報 L D T をポリシー管理サーバ 2 1 に送信する（# 5 5）。

#### 【0080】

営業所において機密情報の機密情報グループを変更または社員の配属を変更する場合は、図 2 1 に示すように、図 6、図 7、または図 8 の各テーブルを更新する（# 6 1）。必要に応じて、暗号化および電子署名の処理をやり直す（# 6 2）。そして、更新されたテーブルをポリシー管理サーバ 2 1 に送信する（# 6

3)。

#### 【0081】

本実施形態によると、システム管理部門が暗号化および電子署名などの情報を一元管理しかつ暗号ポリシーの適用の状況を監視することによって、営業所などの部門ごとに自らの情報を管理しつつ高水準のセキュリティの維持を容易に図ることができる。

#### 【0082】

また、従来のシステムであれば、外部からの不正なアクセスがあった場合に、その機関で取り扱う情報の内容を改ざんされてしまう可能性があった。その機関に属する職員が情報を改ざんする可能性もないとは言えない。これに対して、本実施形態によると、電子署名の処理を適宜やり直すことによって、従来よりも情報を改ざんしにくくし、機密情報の保護の強化を図ることができる。この場合の処理の実行のタイミングは、暗号化の場合と同様にシステム管理部門が一元管理するので、各営業所にとってシステム管理の負担が軽減される。

#### 【0083】

本実施形態のセキュリティシステム1をアウトソーシングシステムのために適用することも可能である。例えば、情報管理の支援を行うアウトソーシング会社に暗号化支援システム2を設け、その支援を受けたい者は機密情報サーバ31を用意すればよい。これにより、小規模企業（いわゆるSOHO）や個人にとっても、容易に高度なセキュリティを得ることができる。

#### 【0084】

その他、セキュリティシステム1、暗号化支援システム2、情報管理システム3、ポリシー管理サーバ21、機密情報サーバ31の全体または各部の構成、テーブルの内容、暗号方式、署名方式、処理内容、処理順序などは、本発明の趣旨に沿って適宜変更することができる。

（付記1）情報を管理する情報管理システムと、前記情報管理システムにおいて情報の暗号化を行うための支援を行う暗号化支援システムと、を有し、

前記暗号化支援システムには、

情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示

す規則情報を記憶する暗号化規則記憶手段と、

前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する暗号化用データ送信手段と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理情報受信手段と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、

前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、が設けられ、

前記情報管理システムには、

前記暗号化用データを前記暗号化支援システムより受信する暗号化用データ受信手段と、

当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、

当該情報管理システムが管理する情報の暗号化を、前記暗号化データ受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、

前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、

前記暗号化手段によって行われた暗号化についての前記処理情報を前記暗号化支援システムに送信する処理情報送信手段と、が設けられ、

てなることを特徴とするセキュリティシステム。

(付記 2) 前記規則情報は、前記規則として、暗号化を行う際に用いる暗号方式と当該暗号化の際に使用する暗号鍵の有効期限とを示し、

前記情報管理システムが情報に暗号化を施した時から現在までの時間が当該情報の区分に対応する前記秘密レベルの前記規則に係る前記有効期限を超えた場合に、

前記警告手段は、当該情報管理システムに対して前記警告を与え、

前記規則情報に示される前記暗号方式が変更された場合に、  
前記暗号化用データ送信手段は、当該変更された暗号方式による暗号化を行うための前記暗号化用データを前記情報管理システムに送信し、  
前記警告手段は、前記警告として、当該変更された暗号方式に従って情報の暗号化を行うべき旨の警告を与える、  
付記1記載のセキュリティシステム。

(付記3) 前記情報管理システムには、  
当該情報管理システムが管理する情報の区分と当該区分に対応する前記秘密レベルとを示す区分秘密レベル情報を前記暗号化支援システムに送信する区分秘密レベル送信手段が設けられ、

前記監視手段は、情報管理システムより受信した前記処理情報と前記区分秘密レベル情報とを比較することによって前記監視を行う、  
付記1または付記2記載のセキュリティシステム。

(付記4) 情報に対して電子署名を行うための証明書の有効期限を管理する有効期限管理手段を有し、

前記監視手段は、前記証明書の有効期限に基づいて、情報に対して電子署名をやり直す必要があるか否かを監視し、

前記警告手段は、電子署名をやり直す必要があると判別された場合に、当該情報を管理する前記情報管理システムに対して電子署名をやり直すべき旨の警告を与える、

付記1ないし付記3のいずれかに記載のセキュリティシステム。  
(付記5) 暗号化支援システムが提供する、情報の暗号化を行うための支援を受けることによって、情報を管理する情報管理システムであって、  
情報を秘密にしたいレベルである秘密レベルごとに定められた、情報の暗号化の規則を示す規則情報と、当該規則に従って情報の暗号化を行うために必要なデータである暗号化用データとを、前記暗号化支援システムより受信する受信手段と、

当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、

当該情報管理システムが管理する情報の暗号化を、前記受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、

前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、

前記規則に従って情報の暗号化が行われたか否かのチェックを受けるために、前記暗号化手段によって行われた暗号化の処理の内容を示す処理情報を前記暗号化支援システムに送信する処理情報送信手段と、

が設けられてなることを特徴とする情報管理システム。

(付記6) 情報を管理する情報管理システムに対して情報の暗号化を行うための支援を行う暗号化支援システムであって、

情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示す規則情報を記憶する暗号化規則記憶手段と、

前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する送信手段と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する受信手段と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、

前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、

が設けられてなることを特徴とする暗号化支援システム。

(付記7) セキュリティ情報提供手段より受信した、セキュリティの脆弱性に関する脆弱性情報に基づいて、現在用いられている暗号化の規則の妥当性を監視する妥当性監視手段を有し、

前記送信手段は、現在用いられている暗号化の規則の妥当性がないと判別された場合に、当該規則を適切に変更するための前記暗号化用データを前記情報管理システムに送信する、

付記 6 記載の暗号化支援システム。

(付記 8) 情報を管理する情報管理システムに対して情報の暗号化を行うための支援を行うコンピュータに用いられるコンピュータプログラムであって、

情報を秘密にしたいレベルである秘密レベルごとの、情報の暗号化の規則を示す規則情報と当該規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する処理と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う処理と、

前記監視によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える処理と、

をコンピュータに実行させるためのコンピュータプログラム。

【0 0 8 5】

【発明の効果】

本発明によると、部門ごとに自らの情報を管理しつつ、高水準のセキュリティの維持を容易に図ることができる。

【図面の簡単な説明】

【図 1】

本発明に係るセキュリティシステムの構成の例を示す図である。

【図 2】

機密情報サーバのハードウェア構成の例を示す図である。

【図 3】

機密情報サーバの機能的構成の例を示す図である。

【図 4】

ポリシー管理サーバの機能的構成の例を示す図である。

【図 5】

暗号化リンクテーブルの例を示す図である。

【図 6】

機密情報グループテーブルの例を示す図である。

【図 7】

部署メンバーテーブルの例を示す図である。

【図 8】

署名期限テーブルの例を示す図である。

【図 9】

作成データ管理テーブルの例を示す図である。

【図 1 0】

システム管理部門が有する例外属性テーブルの例を示す図である。

【図 1 1】

ある営業所が有する例外属性テーブルの例を示す図である。

【図 1 2】

顧客連絡先テーブルの例を示す図である。

【図 1 3】

検針情報テーブルの例を示す図である。

【図 1 4】

料金支払テーブルの例を示す図である。

【図 1 5】

暗号化および電子署名の処理の手順の例を示す図である。

【図 1 6】

暗号化および電子署名の処理の流れの例を説明するフローチャートである。

【図 1 7】

システム管理部門側の準備の処理の流れの例を説明するフローチャートである。

。

【図 1 8】

営業所側の準備の処理の流れの例を説明するフローチャートである。

【図 1 9】



運用開始後の処理の流れの例を説明するフローチャートである。

【図 2 0】

機密情報へのアクセス要求があった場合の機密情報サーバにおける処理の流れの例を説明するフローチャートである。

【図 2 1】

各種設定の変更があった場合の機密情報サーバにおける処理の流れの例を説明するフローチャートである。

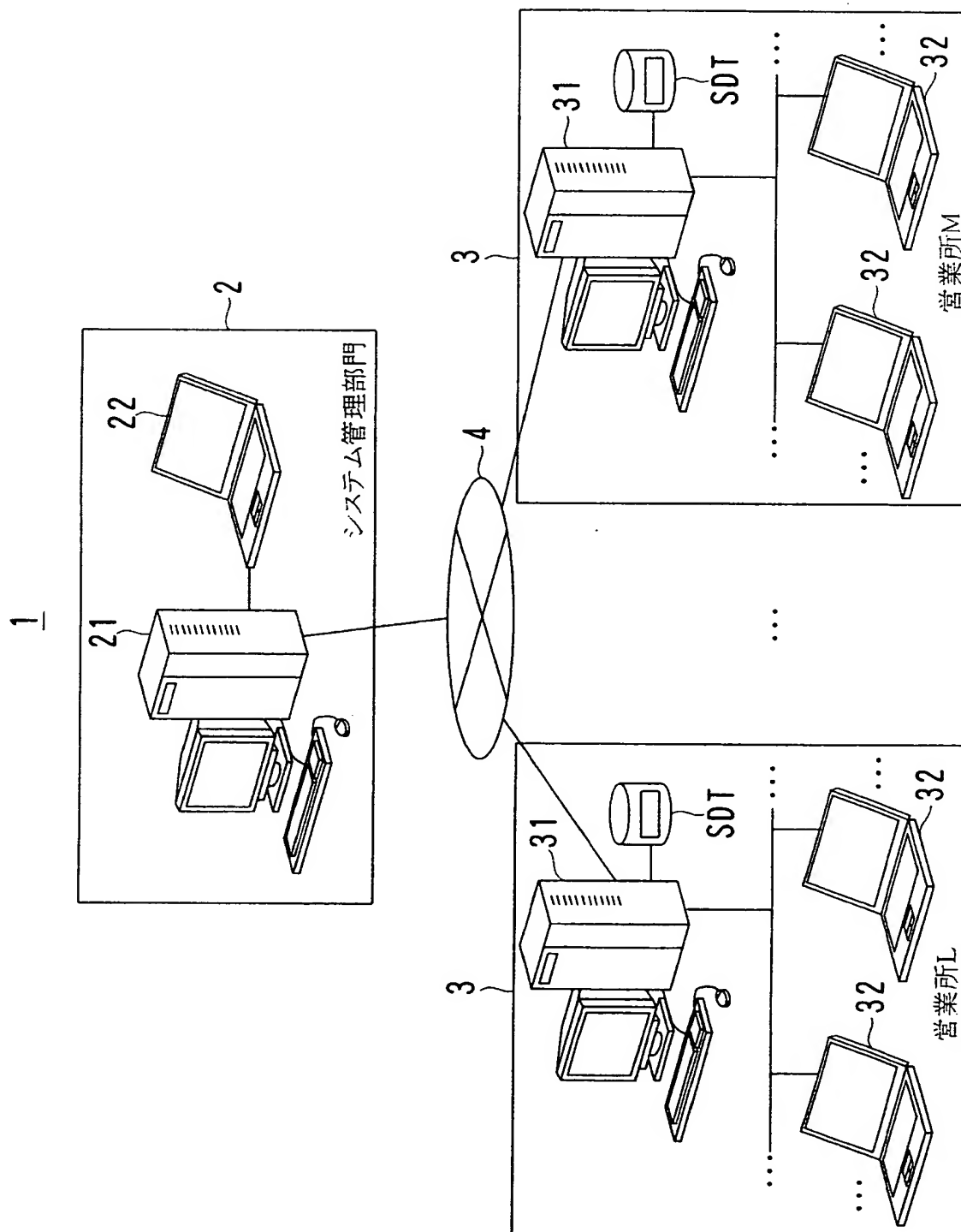
【符号の説明】

- 1 セキュリティシステム
- 2 暗号化支援システム
- 3 機密情報管理システム（情報管理システム）
- 2 0 2 ポリシー情報配付部（暗号化用データ送信手段、送信手段）
- 2 0 3 適用状況監視部（処理情報受信手段、監視手段、受信手段）
- 2 0 5 適用警告部（警告手段）
- 2 D 1 暗号ポリシーデータベース（暗号化規則記憶手段）
- 3 0 2 ポリシー適用部（暗号化用データ受信手段、受信手段）
- 3 0 3 暗号化実行部（暗号化手段）
- 3 0 4 署名処理実行部（処理情報送信手段）
- 3 0 6 グループ情報通知部（区分別秘密レベル送信手段）
- 3 D 1 暗号ポリシーデータベース（区分別秘密レベル記憶手段）
- 3 D 2 機密情報グループデータベース（区分別秘密レベル記憶手段）
- 3 D 5 機密情報データベース（情報記憶手段）
- D T 1 処理完了情報（処理情報）
- D T 5 暗号化用データ
- S D T 機密データ

【書類名】 図面

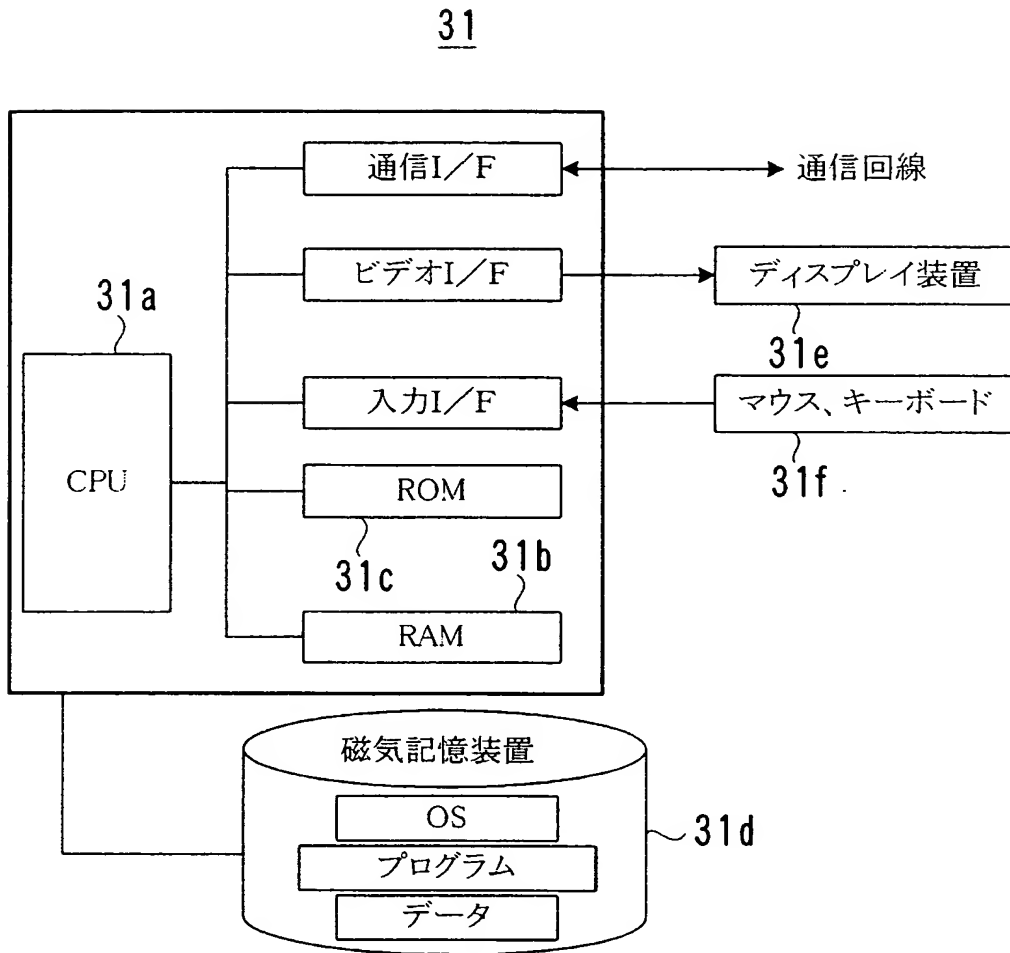
【図 1】

本発明に係るセキュリティシステムの構成の例を示す図



【図 2】

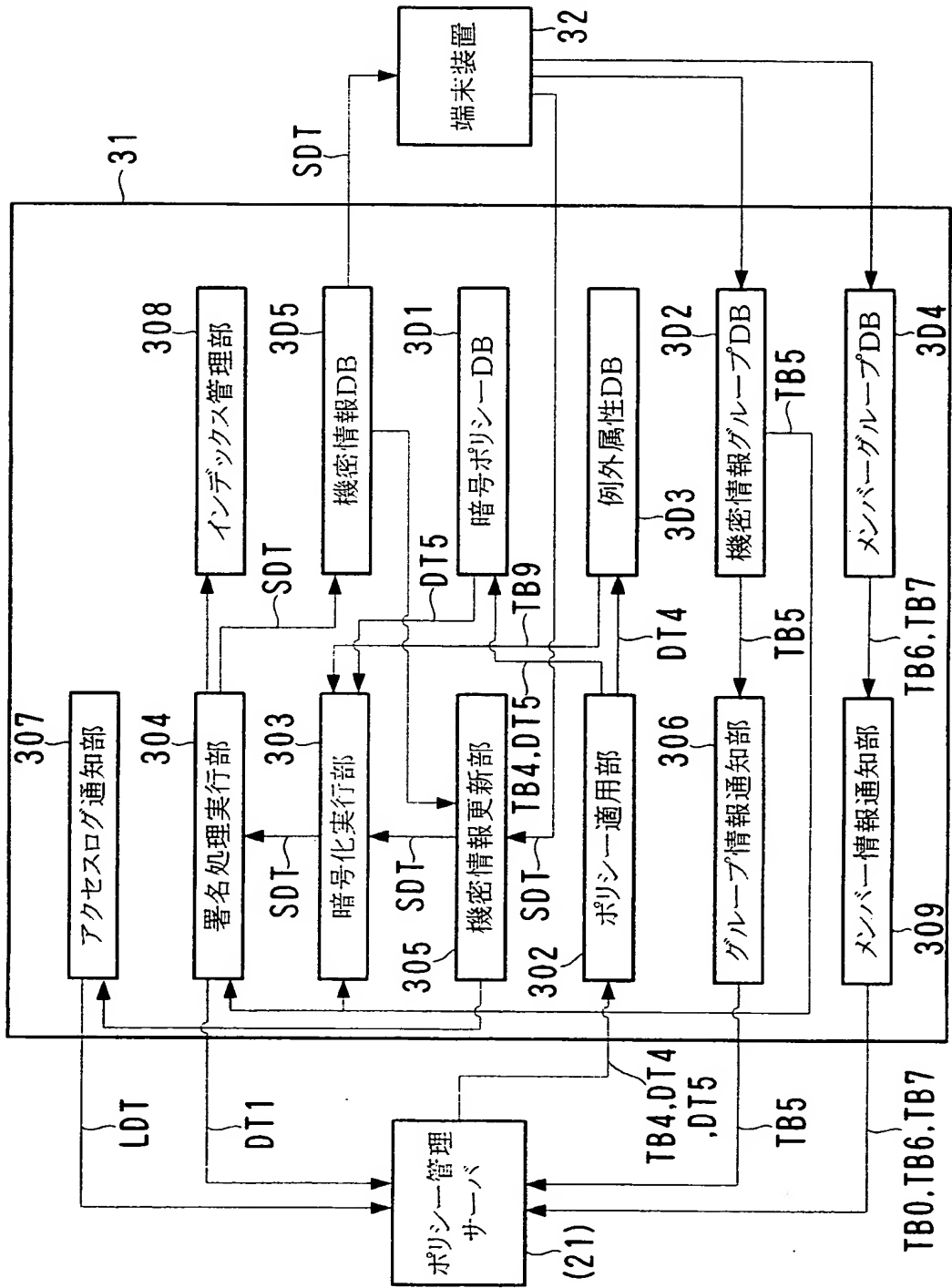
機密情報サーバのハードウェア構成の例を示す図



【図 3】

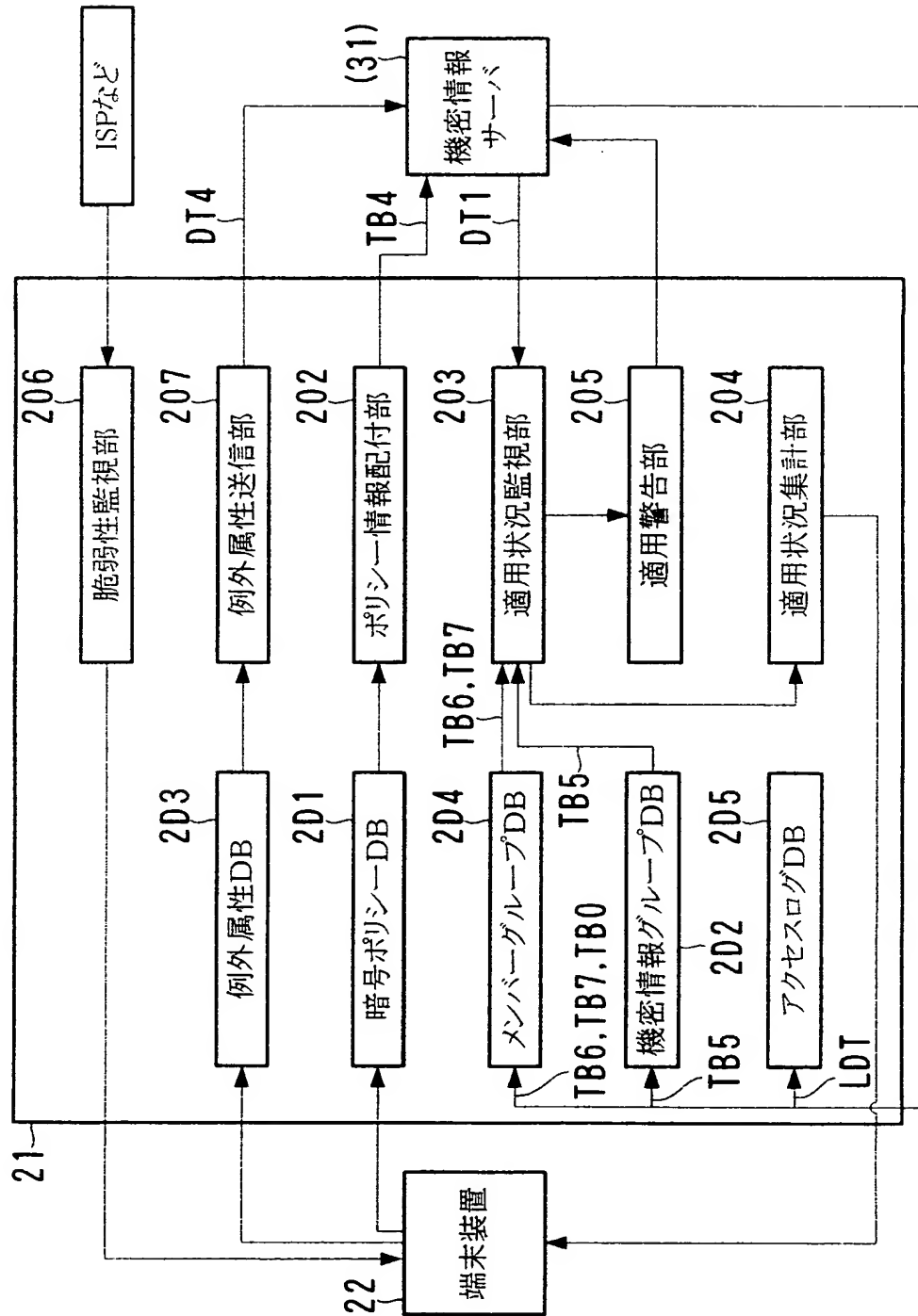
機密情報サーバの機能的構成の例を示す図

3



【図 4】

ポリシー管理サーバの機能的構成の例を示す図



【図 5】

暗号化ランクテーブルの例を示す図

TB4

暗号化 ランク	暗号方式	更新頻度 (有効期限)	機密情報(区分)
A	$\alpha$ 暗号方式	60日	他社秘密情報(秘密度=高)
B	$\beta$ 暗号方式	600日	社内人事情報
C	$\gamma$ 暗号方式 or $\sigma$ 暗号方式	無期限	顧客情報
D	$\beta$ 暗号方式	無期限	内線番号一覧情報 他社秘密情報(秘密度=低)
⋮	⋮	⋮	⋮

【図 6】

機密情報グループテーブルの例を示す図

TB5

サーバ ID	サーバの ある営業所	機密情報 グループ	暗号化 ランク	利用者 グループ	機密情報の区分 (格納場所)	暗号 方式	暗号化 ビット数	レコード 数
S001	営業所M	G1	C	第1課 (顧客窓口)	検針情報テーブル 料金支払いテーブル	$\sigma$ 暗号方式	128bit	100
S001	営業所M	G2	B	第2課 (人事課)	社内人事情報テーブル	$\beta$ 暗号方式	256bit	50
S001	営業所M	G3	C	第3課 (開発課)	ソースファイルディレクトリ	$\sigma$ 暗号方式	128bit	100
S002	営業所L	G4	A	第4課 (営業課)	プレゼン用ディレクトリ	$\alpha$ 暗号方式	256bit	25
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図 7】

部署メンバーテーブルの例を示す図

TB6

サーバ ID	利用者グループ (部署)	メンバー1 (社員1)	メンバー2 (社員2)	...
S001	第1課	鈴木 ○朗	山田 △子	...
	第2課	田中 ○夫	吉田 △子	...
	⋮	⋮	⋮	

【図 8】

署名期限テーブルの例を示す図

TB7

サーバID	利用者グループ (部署)	メンバー (社員)	有効期限	署名方式	署名ビット数
S001	第1課	鈴木 ○朗	2005/11/30	RSA	1024bit
	第1課	山田 △子	2006/06/30	RSA	1024bit
	⋮	⋮	⋮	⋮	⋮



【図 9】

作成データ管理テーブルの例を示す図

TB0a(TB0)

鈴木 〇郎

サーバ ID	機密情報 グループ	文書ID
S001	G1	004
S001	G1	077
S001	G3	200
⋮	⋮	⋮

TB0b(TB0)

山田 △子

サーバ ID	機密情報 グループ	文書ID
S001	G2	076
S001	G3	203
⋮	⋮	⋮

⋮

【図 10】

システム管理部門が有する例外属性テーブルの例を示す図

TB8

営業所 (部門)	機密情報の 区分	暗号化 ランク
営業所M	社内人事情報 テーブル	A
営業所L	検針情報 テーブル	A
全社	料金支払 テーブル	A
⋮	⋮	⋮

【図 1 1】

ある営業所が有する例外属性テーブルの例を示す図

TB9

機密情報の 区分	暗号化 ランク	
社内人事情報 テーブル	A	DT4
料金支払 テーブル	A	DT4
⋮	⋮	

【図 1 2】

顧客連絡先テーブルの例を示す図

TB1

顧客番号	氏名	住所	電話番号	
A0001	○田 一郎	AA県BB市CC町…	012-345-6789	SDT
A0002	△山 太郎	AA県BB市DD町…	012-345-0000	SDT
⋮	⋮	⋮	⋮	

【図 1 3】

検針情報テーブルの例を示す図

TB2

顧客番号	検針値	
A0001	950kWh	SDT
A0002	815kWh	SDT
⋮	⋮	

【図 1 4】

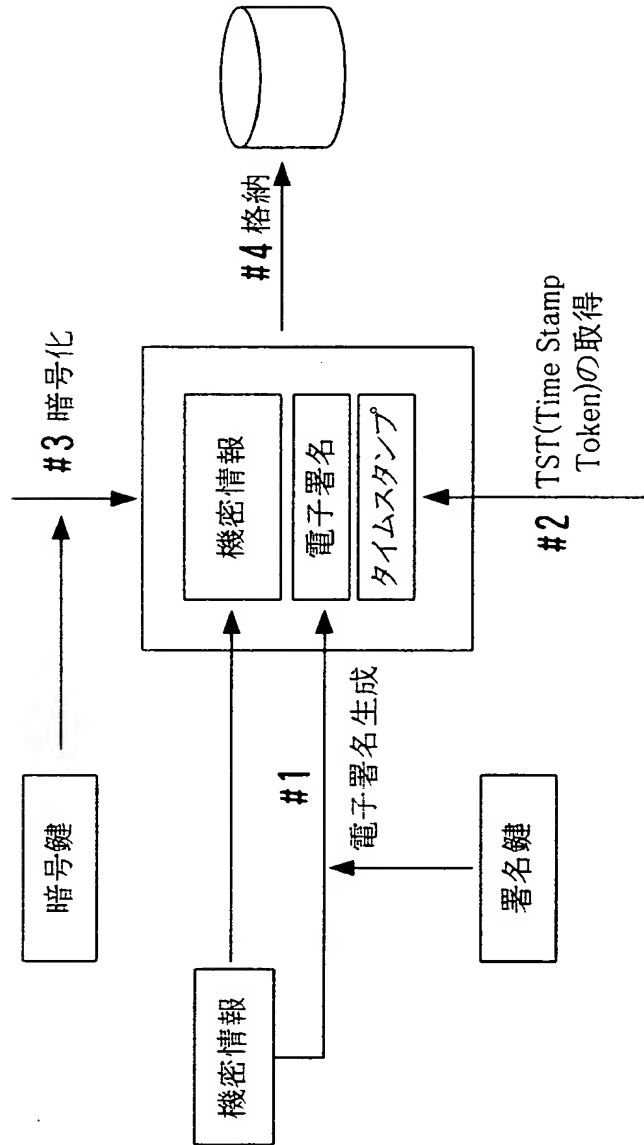
料金支払テーブルの例を示す図

TB3

顧客番号	支払方法	口座番号	
A0001	銀行自動引落し	X銀行Y支店普通012345	SDT
A0002	窓口支払	-	SDT
⋮	⋮	⋮	

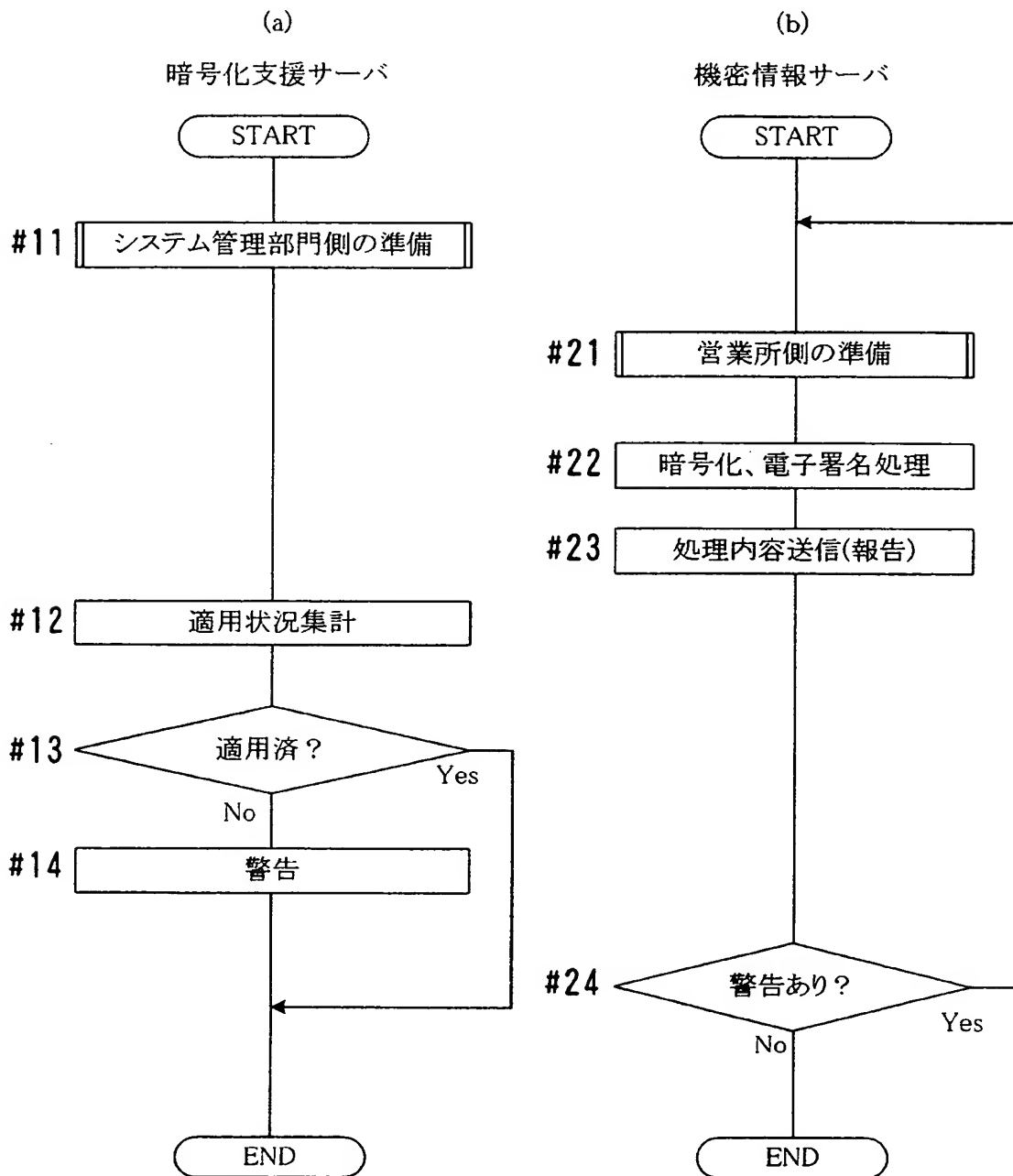
【図 15】

暗号化および電子署名の処理の手順の例を示す図



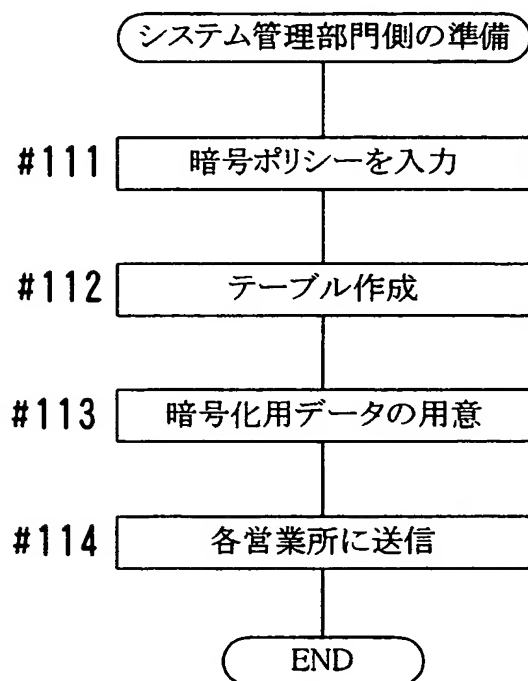
【図 16】

暗号化および電子署名の処理の流れの例を説明するフローチャート



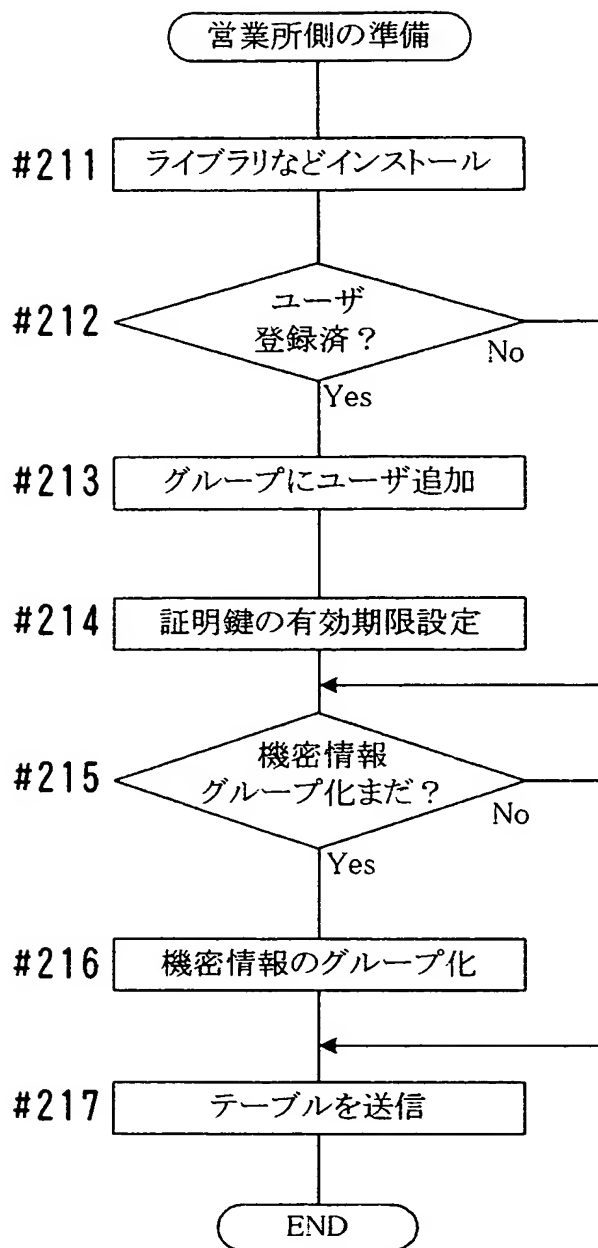
【図 17】

システム管理部門側の準備の処理の流れの例を説明するフローチャート



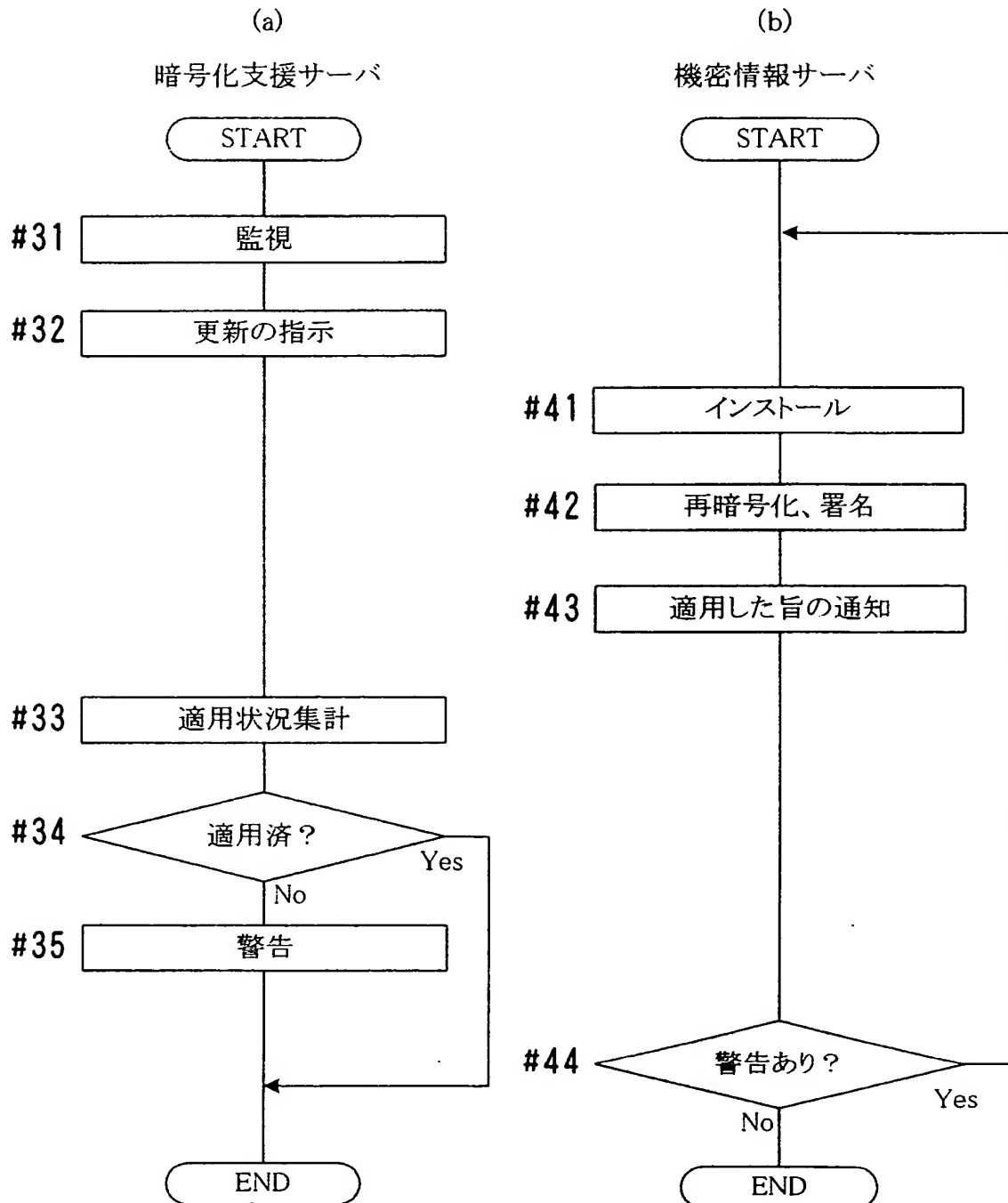
【図 18】

営業所側の準備の処理の流れの例を説明するフローチャート



【図 19】

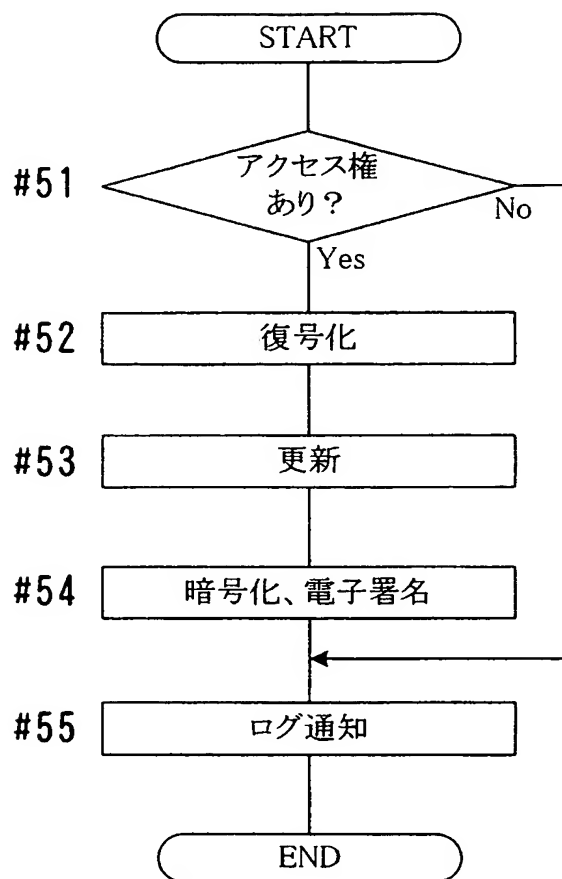
運用開始後の処理の流れの例を説明するフローチャート





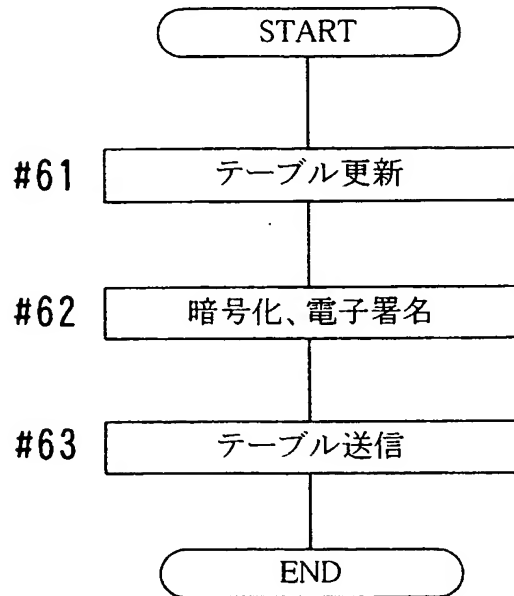
【図 20】

機密情報へのアクセス要求があった場合の機密情報サーバにおける処理の流れの例を説明するフローチャート



【図 2 1】

各種設定の変更があった場合の機密情報サーバにおける  
処理の流れの例を説明するフローチャート



【書類名】 要約書

【要約】

【課題】 部門ごとに自らの情報を管理しつつ、高水準のセキュリティの維持を容易に図る。

【解決手段】 暗号化支援システム 2 は、暗号化の規則を秘密レベルごとに記憶し、規則に従って情報の暗号化を行うために必要な暗号化用データを機密情報管理システム 3 に送信し、機密情報管理システム 3 が行った暗号化の処理の内容を示す処理情報を受信し、機密情報管理システム 3 において規則に従って情報の暗号化が行われているか否かの監視を、その機密情報管理システム 3 より受信した処理情報に基づいて行い、規則に従って情報の暗号化を行っていない情報管理システム 3 に対して警告を与える。機密情報管理システム 3 は、暗号化用データを暗号化支援システム 2 より受信し、自ら管理する情報の区分を秘密レベルと対応付けて記憶し、自ら管理する情報の暗号化をその情報の区分に対応する秘密レベルの暗号化用データを用いて行い、暗号化が施された情報を記憶し、行った暗号化についての処理情報を暗号化支援システム 2 に送信する。

【選択図】 図 1

特願 2 0 0 3 - 0 5 1 8 4 2

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 2 2 3 ]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社